

REMARKS

Claims 1, 10, 12-14, 17, 18, 24, 27, 32, 42, 50, 57 and 62 have been amended to improve form and claims 8, 9, 11, 26, 28, 47, 48 and 51 have been canceled without prejudice or disclaimer. Claims 1-7, 10, 12-19, 21-25, 27, 29, 31-33, 35, 37-46, 49, 50 and 52-69 are now pending in this application.

Claim 17 has been objected to for a minor informality. Claim 17 has hereby been amended to address the objection. Accordingly, withdrawal of the objection is respectfully requested.

Claims 18 and 27 have been rejected under 35 U.S.C. § 112, second paragraph as being incomplete for omitting essential structural cooperative relationship of elements. More particularly, the Office Action indicates that there is no connection between the claimed grouping of IP packets with a method of detecting and preventing security breaches in a network (Office Action – page 3). Claim 18, as amended, recites “A method comprising ...” and claim 27, as amended, recites “A system comprising ...”. The applicants assert that no essential cooperative of relationship of elements exist in amended claims 18 and 27. Accordingly, withdrawal of the rejection of claims 18 and 27 under 35 U.S.C. § 112, second paragraph is respectfully requested.

Claims 1-7, 12-17, 21-25, 31, 33, 35, 37-40, 43-45, 49-50, 52-55, 58, 60 and 63-69 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf et al. (U.S. Patent No. 6,499,107; hereinafter Gleichauf ‘107) and Gleichauf et al. (U.S. Patent No. 6,324,656; hereinafter Gleichauf ‘656 in view of Nikander et al. (U.S. Patent No. 6,253,321; hereinafter Nikander); claims 8-11, 26-28, 32, 41, 47, 48, 51, 56, 61 and 62 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf ‘107 and Gleichauf ‘656 in

view of Nikander and further in view of Copeland III (U.S. Patent Publication No. 2003/0105976; hereinafter Copeland III); claims 19 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 and Gleichauf '656 in view of Nikander and Copeland III and further in view of Alexander et al. (U.S. Patent Publication No. 2004/0258073; hereinafter Alexander); and claims 42, 46, 57 and 59 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 in view of Nikander and further in view of Trcka et al. (U.S. Patent No. 6,453,345; hereinafter Trcka). The rejections are respectfully traversed.

Initially, the applicants note that claims 42 and 57 have been rejected based on the combination of Gleichauf '107, Nikander and Trcka. Claims 43-45, 49, 50, 52-55, 58, 60 and 63-69, which variously depend on claims 42 and 57, have been rejected based on the combination of Gleichauf '107 and Gleichauf '656 in view of Nikander. Therefore, the rejection of these dependent claims is not consistent with the rejection of independent claims 42 and 57. The applicants respectfully request clarification as to the grounds of rejection in any subsequent communication.

Claim 1, as amended, recites that the method includes grouping the plurality of TCP packets into packet flows and sessions and storing the packet flows in packet flow descriptors. Claim 1, as amended, also recites that the inspecting the TCP stream to detect information indicative of a security breach comprises searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream. Similar features were previously recited in claims 8, 9 and 11.

As to these features, the Office Action admits that none of Gleichauf '107, Gleichauf '656 or Nikander discloses these features (Office Action – page 9). The Office Action,

however, states that Copeland III discloses these features and relies upon paragraphs 58-61 and paragraph 70 for support (Office Action – page 9). Copeland III at paragraphs 58-61 discloses that a session is a series of interactions between two communication end points. This portion of Copeland III further discloses that a TCP/IP packet includes a header portion and a data portion. This portion of Copeland III does not disclose or suggest grouping the plurality of TCP packets into packet flows and sessions and storing the packet flows in packet flow descriptors, as alleged in the Office Action.

Copeland III at paragraph 70 discloses that the flow-based engine 155 associates all packets with a flow. Copeland III at paragraph 70 further discloses that engine 155 analyzes certain statistical data and assigns a concern index value to abnormal activity. This portion of Copeland III does not disclose or suggest that inspecting a TCP stream comprises searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream, as alleged in the Office Action.

For at least these reasons, the combination of Gleichauf '107, Gleichauf '656, Nikander and Copeland III does not disclose or suggest each of the features of claim 1. Accordingly, withdrawal of the rejection and allowance of claim 1 are respectfully requested.

Claims 2-7, 10, 12-17, 21 and 23 depend from claim 1 and are believed to be allowable for at least the reasons claim 1 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 2-7, 10, 12-17, 21 and 23 are respectfully requested.

Claims 18, 24 and 27 recite features similar to, but of different scope than claim 1. For reasons similar to those discussed above with respect to claim 1, withdrawal of the rejection and allowance of claims 18, 24 and 27 are respectfully requested.

Claims 25, 31, 33, 35, 37, 38, 40 and 41 depend from claim 24 and are believed to be allowable for at least the reasons claim 24 is allowable. Claim 32 depends from claim 27 and is believed to be allowable for at least the reasons claim 27 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 25, 31-33, 35, 37, 38, 40 and 41 are respectfully requested.

Claim 22 recites querying a signatures database to determine whether there are matching signatures in the TCP stream using deterministic finite automata for pattern matching. Claim 39 recites a similar feature. The Office Action admits that Gleichauf '107, Gleichauf '656 and Nikander do not disclose these features, but takes Official Notice that employing "the use of deterministic finite automaton for providing a pattern matching is well known in the theory of computation in the system of Gleichauf and Nikander so as to effectively implementing pattern matching" (Office Action – page 7-8). The applicants respectfully disagree and assert that using deterministic finite automata to determine whether there are matching signatures in a TCP stream and a signatures database is not well known. The applicants respectfully request that any subsequent Office Action produce a reference that discloses the use of deterministic finite automata in the manner recited in claims 22 and 39 or withdraw the rejection.

For at least these reasons, the combination of Gleichauf '107, Gleichauf '656 and Nikander does not disclose or suggest each of the features of claims 22 and 39. Accordingly, withdrawal of the rejection and allowance of claims 22 and 39 are respectfully requested.

Claims 19 and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 and Gleichauf '656 in view of Nikander and Copeland III and further in view of Alexander. The rejection is respectfully traversed.

Claims 19 and 29 are dependent on claims 18 and 27, respectively, and are believed to be allowable for at least their respective independent claims are allowable. Alexander does not remedy the deficiencies in the combination of Gleichauf '107, Gleichauf '656, Nikander and Copeland III discussed above with respect to claims 18 and 27. Accordingly, withdrawal of the rejection and allowance of claims 19 and 29 are respectfully requested.

Claims 42, 46, 57 and 59 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Gleichauf '107 in view of Nikander and further in view of Trcka. The rejection is respectfully traversed.

Claims 42 and 57, as amended, recite features similar to, but not identical to claim 1. For reasons similar to those discussed above with respect to claim 1, the combination of Gleichauf '107 and Nikander does not disclose each of the features of amended claims 42 and 57. In addition, neither Trcka nor Copeland III remedies the deficiencies in the combination of Gleichauf '107 and Nikander discussed above with respect to claim 1. Accordingly, withdrawal of the rejection and allowance of claims 42 and 57 are respectfully requested.

Claims 43-46, 49, 50 and 52-56 are dependent on claim 42 and are believed to be allowable for at least the reasons claim 42 is allowable. Claims 58-69 depend from claim 57 and are believed to be allowable for at least the reasons claim 57 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 43-46, 49, 50, 52-56 and 58-69 are respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, the applicants respectfully request withdrawal of the outstanding rejections and the timely allowance of this application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY & SNYDER, L.L.P.

By: /Glenn Snyder/
Glenn Snyder
Reg. No. 41,428

Date: August 7, 2006

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808